

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Kenji OHKUMA, et al.

SERIAL NO: NEW APPLICATION

GAU:

FILED: HEREWITH

EXAMINER:

FOR: ENCRYPTION APPARATUS AND METHOD, AND DECRYPTION APPARATUS AND METHOD BASED ON BLOCK ENCRYPTION



INFORMATION DISCLOSURE/RELATED CASE STATEMENT UNDER 37 CFR 1.97

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

SIR:

Applicant(s) wish to disclose the following information.

REFERENCES

- ☒ The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references are attached, where required, as are either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

RELATED CASES

- ☒ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- ☐ A check is attached in the amount required under 37 CFR §1.17(p).

CERTIFICATION

- ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

DEPOSIT ACCOUNT

- ☒ Please charge any additional fees for the papers being filed herewith and for which no check is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Marvin J. Spivak  
Registration No. 24,913

C. Irvin McClelland  
Registration Number 21,124



22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 10/98)



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Kenji OHKUMA, et al.

SERIAL NO.: NEW APPLICATION

FILED: HERewith

FOR: ENCRYPTION APPARATUS AND METHOD, AND  
DECRYPTION APPARATUS AND METHOD BASED ON  
BLOCK ENCRYPTION

**STATEMENT OF RELEVANCY**

**References AR through AZ on form PTO-1449:**

These references are referred to in the body of the specification.

**Reference AU (The Block Cipher SQUARE) on for PTO-1449:**

This paper shows an SPN structure where the diffusion layer consists byte shift operations and a locally MDS diffusions. We found that its multiple-round structure can be equivalently transformed into a recursive SPN structure. But the authors did not refer to the hierarchical structure. (Figure 1 and lines 15-20 of page 151)

**Reference AV (AES Proposal: Rijndael) on for PTO-1449:**

Rijndael is a very similar algorithm to the cipher Square. This paper shows an SPN structure where the diffusion layer consists of byte shift operations and a locally MDS diffusions. We found that its multiple-round structure can be transformed into a recursive SPN structure. But the authors did not refer to the hierarchical structure. (Lines 3-9 of Section 4.2 of page 10)

**Reference AW (Handbook of Applied Cryptography) on for PTO-1449:**

This reference is a standard textbook which covers broad aspects of cryptography. We could not find any description on structures similar to the nested SPN structure there in the reference.

**Reference AX (Applied Cryptography) on for PTO-1449:**

This reference is a standard textbook which covers broad aspects of cryptography. We could not find any description on structures similar to the nested SPN structure there in the reference.

**Reference AY (The block cipher Hierocrypt) on for PTO-1449:**

This paper was written by the inventors of the present application. It proposes a nested SPN structure (Figure 1 in page 71, and 5<sup>th</sup> paragraph of “1 Introduction” in page 70) But the multiple-path condition is not mentioned in this paper.

**Reference AZ (Security and Performance Evaluations for the block ciphers Hierocrypt-3 and Hierocrypt-L1 ) on for PTO-1449:**

This paper was written by the inventors of the present application. It defines the multiple-path condition (3<sup>rd</sup> paragraph of subsection “3.2.3 MDS<sub>H</sub>” in page 75) and proposes a block cipher under the condition (1<sup>st</sup> paragraph of 3.2.3 MDS<sub>H</sub> in page 75).

**LIST OF RELATED CASES**

<u>Docket Number</u>	<u>Serial or Patent No.</u>	<u>Filing or Issue Date</u>	<u>Status or Patentee</u>
204301US2SRD	09/799,028	03/06/01	PENDING

GJM/ae

Form PTO 1449  
(Modified)U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE

ATTY DOCKET NO.

210580US2SRD

SERIAL NO.

NEW APPLICATION

LIST OF REFERENCES CITED BY APPLICANT

APPLICANT

Kenji OHKUMA, et al.

FILING DATE

HEREWITH

GROUP

## U.S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						

## FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES	NO
	AO					
	AP					
	AQ					

## OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)

AR	V. RIJMEN, et al., "The Cipher SHARK", Fast Software Encryption, LNCS 1039, 1996, pgs. 100-111
AS	Kazumaro AOKI, et al., "Stricter Evaluation for the Maximum Average of Differential Probability and the Maximum Average of Linear Probability", SCIS 96-4A, 1996, 12 pages
AT	Mitsuru MATSUI, "Block Encryption Algorithm MISTY", ISEC 96-11, 1996, pgs 1-14
AU	J. DAEMEN, et al., "The Block Cipher SQUARE", Fast Software Encryption, 1997 (FSE97), LNCS 1267, pgs. 149-165
AV	J. DAEMEN, et al., "AES Proposal: Rijndael", Document Version 2, 1999, pgs. 1-45
AW	A.J. MENEZES, et al., Handbook of Applied Cryptography, CRC Press, 1996, 11 pages
AX	B. SCHNEIER, Applied Cryptography, Second Edition, 1995, 10 pages
AY	K. OHKUMA, et al., "The block cipher Hierocrypt", Proceedings of Selected Area in Cryptography 2000 (SAC 2000), 2000, pgs 70-82
AZ	K. OHKUMA, et al., "Security and Performance Evaluations for the block ciphers Hierocrypt-3 and Hierocrypt-L1", Technical Report of IEICE, ISEC-71, 2000(Japan), 2001, pgs. 71-100

Examiner

Date Considered

\*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

09/893785  
06/29/01